CI August 4, 1998

MEMORANDUM FOR DISTRIBUTIION

SUBJECT: CIO Letter 98-3, Year 2000 Business Continuity and Contingency Planning

This policy letter issues guidance for Year 2000 (Y2K) contingency planning. The objective is to have plans in place to ensure the continuation of core business processes in the event of Information Technology failures caused by Y2K problems in application software, systems software, embedded microcircuit code, and the like. Last year contingency plans were developed for DLA mission critical areas and a few areas of special interest. You are requested to review and update the plans in accordance with the guidance in this correspondence.

Contingency planning has assumed greater importance in the Department of Defense Y2K strategy. Planners and managers fear that not all program code will be fixed and tested in time. We know from experience that not all programs work perfectly when first installed. The new version of the Department of Defense Year 2000 Management Plan will greatly expand the coverage of contingency planning. It will require DoD Components to develop and maintain plans to ensure the continuity of their core business processes focusing on their operational missions.

The focus of DLA Y2K contingency planning is on business process continuity. It is not continuity of operations. If a system does not work because of a Y2K software problem, it will not work at the COOP site either. Also, the problem extends beyond automated information systems and the information systems infrastructure to the facilities infrastructure, which is in the realm of business continuity.

There are two excellent publications available as helpful guides. General Accounting Office exposure draft Year 2000 Computing Crisis: Business Continuity and Contingency Planning is available at http://www.gao.gov/special.pubs/publist.htm. The Social Security Administration Year-2000 Business Continuity and Contingency Plan is included in the draft Department of Defense Year 2000 Management Plan as Appendices H.4 (narrative) and H.5 (tables), available at http://www.disa.mil/cio/y2k/manplan.html.

All Y2K business continuity and contingency planning efforts should follow a similar methodology. The plan documenting the planning effort should describe how you will operate if the supporting IT systems fail. The level of risk will determine size and the amount of detail in the plan. The following policies are in effect for DLA organizations for Y2K business continuity and contingency planning:

a. Review all your business processes, and develop business continuity and contingency plans based on their mission essentiality. Identify the IT -- the standard and unique business applications, the information systems infrastructure, and the facilities and equipment -- supporting each process, and assess each process's vulnerability to an IT failure.

b. Do a risk analysis that describes the mission essentiality of each process and its vulnerability. If a process is mission essential and dependent on IT, explore realistic alternative ways to do it.

c. If there are large-system failures, they will need to be resolved quickly in an orderly fashion. Prioritize the processes based on mission essentiality and vulnerability as a guide to allocating resources in case you are overwhelmed with failures. Devise strategies for bringing systems back on line, such as forming Tiger Teams or Rapid Response Teams. Consider using COOP Quick Response Teams as a resource to facilitate resumption.

d. Team with the organizations that maintain your applications and facilities and the organizations that run them. Make sure they know what your priorities are so they can allocate their resources accordingly. Develop mutual strategies on how you will transition to the year 2000. Address issues such as: whether to stop data processing operations just before midnight and resume just after midnight or to continue without interruption; how and when to take safety dumps; when to produce year end reports -- before the end of the year or normally; whether or not to freeze system changes toward the end of the year.

e. Identify the funding resource requirements and personnel skills required to implement the plan.

f. Test the plan to determine its feasibility and to ensure that all the players know their roles.

Please complete your efforts and submit completed plans to us by the end of November 1998. My point of contact for this matter is Ms. Sandra King at DSN 427-2141 and sandra_king@hq.dla.mil.

//S//
CARLA A. VON BERNEWITZ
Chief Information Officer